UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/612,982	07/10/2000	David Moshe Goldschlag	1999-32	9438

23823 7590 12/31/2003

Digital Video Express, LP
1408 BAYSHIRE LANE
Herndon, VA 20170

EXAMINER	
TRAN, TONGOC	
ART UNIT	PAPER NUMBER
2134	4

DATE MAILED: 12/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/612,982	GOLDSCHLAG ET AL.	
	Examiner	Art Unit	
	Tongoc Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *10 July 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

1. This office action is in response to applicants' application serial no. 09/612982 filed on 7/10/2000.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claim 17 recites the limitation "said set top box records" in line 1. There is insufficient antecedent basis for this limitation in the claim. For the purpose of prosecuting the case, "said set top box records" is considered to be "trusted device records" as recited in claim 14.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sims, III (U.S. Patent No. 6,438,235 hereinafter Sims) and Eldridge et al. (U.S. Patent No. 6,094,721 hereinafter Eldridge) in view of de Silva et al. (U.S. Patent No. 6,615,347 hereinafter de Silva).

In respect to claim 1, Sims discloses a method for protection of content stored in a trusted device comprising the steps of:

(a) receiving keying information from a manufacturer, said manufacturer having received said keying information from a licensing authority (see Sims, col. 2, lines 44-62);

Sims discloses generating private key and a public key (see Sims, col. 4, lines 48-64) but does not explicitly discloses:

(b) generating a temporary private key;

(c) computing a final private key using said temporary private key and said keying information;

(d) computing a final public key using said temporary private key and said keying information.

However, Eldridge discloses (a) a private key is generating using a temporary key (a password), (b) computing a final private key using a temporary private key (a password) and keying information (a sequence number identifying password, a randomly-generated number or other data associated with a client process), (c) computing a final public key using said temporary private key and said keying information (see Eldridge, col. 5, lines 33-52). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Sims' teaching of generating a private and a public key with Eldridge's teaching of associating password with generation private and public keys for a more secure access control by associating password with a client process results in a generation of a new key and a new key identifier (see Eldridge, col. 1, lines 49-54).

Furthermore, Sims does not disclose:

(e) sending said final public key to said manufacturer for certification; and

(f) receiving a binding certificate from said manufacturer.

However, de Silva discloses sending a public key to a certification authority and receiving a binding certificate from said authority (see de Silva, col. 3, lines 25-35). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Sims' teaching of generating a public and private key with de Silva's teaching of sending the public key for certification and receiving a binding certification from a certificate authority because one of the purpose of the digital certificate is to document in a trustworthy manner that the public key is associated with the party that holds the public key (see col. 1, lines 45-47).

In respect to claim 2, Sims, Eldridge and de Silva disclose the method according to claim 1, wherein said keying information includes an initial private key and an identifier (see Eldridge, col. 5, lines 33-53).

In respect to claim 3, Sims, Eldridge and de Silva disclose the method according to claim 2, further including the step of forgetting the initial private key (see Eldridge, col. 5, lines 33-53, password).

In respect to claim 4, Sims, Eldridge and de Silva disclose the method according to claim 1, further including the step of computing an evidentiary certificate (see de Silva, col. 5, lines 14-41).

In respect to claim 5, Sims, Eldridge and de Silva disclose the method according to claim 4, wherein said evidentiary certificate includes text and a signature of the text (see de Silva, col. 5, lines 14-41).

In respect to claim 6, Sims, Eldridge and de Silva disclose the method according to claim 4, further including the step of recording public keys on playback devices (see Sims, col. 10, lines 40-55) but does not explicitly discloses said presenting a copy of said evidentiary certificate to a second device. However, authorizing multiple copies of usages as part of a licensing agreement is old and well known. It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Sims' recording public keys in multiple devices with de Silva's teaching of associating digital certificate with a public key for the benefit of using the same copy of digital certificate associating with the same public key for all the devices instead of associating multiple certificate with multiple public keys for multiple devices.

In respect to claim 7, Sims, Eldridge, and de Silva disclose the method according to claim 4, further including the step of said second device verifying the public keys (see Sims, col. 10, lines 40-55).

In respect to claim 8, Sims, Eldridge, and de Silva disclose the method according to claim 6, further including the steps of:

(a) said second device requesting a credential confirmation from said trusted device (see de Silva, col. 4, lines 33-51, certificate issuer engine and subscriber or user's system);

(b) said trusted device computing a credential confirmation (see de Silva, col. 5, lines 15-40); and

(c) said trusted device presenting a copy of said credential certificate to said second device (see de Silva, col. 5, lines I3-18).

In respect to claim 9 and 10, Sims, Eldridge and de Silva disclose the method according to claim 4 further but does not explicitly discloses presenting a copy of said evidentiary certificate to said licensing authority and said licensing authority verifying said evidentiary certificate. However, de Silva discloses secret protocol for encryption of data and the generation of keys is only revealed by license i.e., only trusted manufacturers of content and devices...see Sims, col. 2, lines 44-62). Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Sims' teaching of sharing secret protocol of encryption of data between trusted manufacturers of content and device by presenting a copy of said evidentiary certificate to said licensing authority (trusted manufacturer of content) and said licensing authority verifying said evidentiary certificate to ensure that certain public key corresponds to a certain entity.

In respect to claim 11, Sims, Eldridge and de Silva do not disclose the method according to claim 10 wherein said step of said licensing authority verifying said evidentiary certificate further includes the steps of

(a) recomputing the final public key from the keying information and the evidentiary certificate; and

(b) checking that the recomputed final public key with a manufacture's certificate.

However, Sims discloses sharing secret protocol for encryption of data and the generation of keys between the trusted manufacturers of content and devices (see Sims, col. 2, lines 44-62) and provider of content compiles a list of user or decoders

and/or play-back devices authorized to utilize the content of the media and this list includes both the identification of user or decoders as well as their public keys (see Sims, col. 14, lines 35-39). Furthermore, de Silva discloses the digital certificate includes a serial number...the subscriber's distinguished name, subscriber's public key...see de Silva, col. 5, lines 15-40). Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Sims' teaching of generating a list of authorized content users or decoders with their public keys by the content provider and de Silva's teaching of digital certificate's content to incorporate the verifying steps of (a) recomputing the final public from the keying information and the evidentiary certificate and (b) checking the recomputed final public key with a manufacture's certificate (trusted manufacture of devices) to ensure that the information provided in the certificate correspond to the information of the authorized content user list.

In respect to claim 12, Sims, Eldridge and de Silva disclose the method according to claim 8, wherein said step of computing a credential confirmation includes using a hash function (see de Silva, col. 5, lines 35-41).

In respect to claim 13, Sims disclose an apparatus for manufacturing trusted devices comprising:

(a) a licensing authority for providing keying information (b) a multitude of manufactures, each of said manufactures receiving keying information from the licensing authority (see Sims, col. 2, lines 44-62).

(c) a multitude of trusted devices, each of said trusted devices receiving keying information from one of said multitude of manufacturers (see Sims, col. 2, lines 44-63)

Sims discloses generating a final private trusted device key and final public trusted device key but does not explicitly discloses said private and public keys are using said keying information.

However, Eldridge discloses generating a public and private key using keying information (i.e. data derived from password...see Eldridge, col. 5, lines 33-53). It would have been obvious to one of ordinary skill in the art at the time the invention was made to implement Sims' teaching of generating a private and a public key with Eldridge's teaching of associating password with generation of public and private keys for a more secure access control by associating password with a client process results in a generation of a new key and a new key identifier (see Eldridge, col. 1, lines 49-54).

Furthermore, Sims does not disclose wherein said manufacture certifies said public trusted devices key.

However, de Silva discloses sending a public key to a certification authority and receiving a binding certificate from said authority (see de Silva, col. 3, lines 25-35). It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Sims' teaching of generating a public and private key with de Silva's teaching of sending the public key for certification and receiving a binding certification from a certificate authority because one of the purpose of the digital certificate is to document in a trustworthy manner that the public key is associated with the party that holds the public key (see de Silva, col. 1, lines 45-47).

In respect to claim 14, Sims, Eldridge and de Silva disclose an apparatus according to claim 13, wherein said licensing authority includes a database, said database containing trusted device records (see Sims, col. 14, lines 35-39).

In respect to claim 15, Sims, Eldridge and de Silva disclose an apparatus according to claim 14, wherein said trusted device records include a public key (see Sims, col. 14, lines 35-40).

In respect to claim 16, Sims, Eldridge and de Silva disclose an apparatus according to claim 14, wherein said trusted device records include:

(a) a trusted device identifier; (b) a manufacturer identifier (see Sims, col. 14, lines 35-40).

In respect to claim 17, Sims, Eldridge and de Silva disclose an apparatus according to claim 14, wherein said trusted device records include a set top box public key (see Sims, col. 10, lines 40-55).

In respect to claim 18, Sims, Eldridge and de Silva disclose an apparatus according to claim 14, wherein said trusted device records include a manufacturer's public key (see Sims, col. 14, lines 35-40) but does not explicitly discloses said trusted device records include a manufacturer certificate. However, de Silva disclose using digital certificate to verify the owner of the public key (see de Silva, col. 1, lines 40-54). It would have been obvious to one of ordinary skill in the art at the time the invention was made include the manufacturer certificate in the trusted device records taught by Sims with verifying the owner of the public key with digital certificate taught by de Silva

for the benefit of ensuring that the public key in the trusted device is indeed belongs to the manufacture that issue it.

In respect to claim 19, Sims, Eldridge and de Silva disclose an apparatus according to claim 14, wherein said trusted device records include a communications identifier for identifying a device with which the trusted device may communicate (see Sims, col. 21, lines 10-30).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

-Gruise et al. Disclose a key management system for digital content player.

-Hurtado et al. Disclose a multimedia player for an electronic content delivery system.

-Sudia et al. disclose a multi-step digital signature method and system.

-Shimizu et al. Disclose an information processing system having function of securely protecting confidential information.

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tongoc Tran whose telephone number is (703) 305-7690. The examiner can normally be reached on 8:30-5:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A. Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 746-7240.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703)305-9600.

Examiner Tongoc Tran
Art Unit: 2134

TT
December 24, 2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100